

UNITED STATES DISTRICT COURT  
FOR THE  
DISTRICT OF VERMONT

2013 AUG -7 PM 3: 59

CLERK  
*PC*  
BY \_\_\_\_\_  
DEPUTY CLERK

UNITED STATES OF AMERICA     )  
  )  
  )  
  )  
  )  
FRANK CARABALLO                )

Case No. 5:12-cr-105

**OPINION AND ORDER DENYING DEFENDANT'S MOTION TO SUPPRESS  
EVIDENCE BASED ON THE GOVERNMENT'S WARRANTLESS USE OF  
REAL-TIME CELL PHONE LOCATION INFORMATION**

(Doc. 38)

This matter came before the court on Defendant's Motion to Suppress Evidence Based on the Government's Warrantless Use of Real-Time Cell Phone Location Information. (Doc. 38). Defendant contends that the government's warrantless search of his cell phone violated his Fourth Amendment rights. The government opposes the motion, contending that no search occurred and that if it did, it was justified by exigent circumstances, a reasonable good faith understanding of the applicable law, the automobile exception, and the inevitable discovery doctrine.

The government is represented by Assistant United States Attorney Joseph R. Perella, and Assistant United States Attorney Paul J. Van de Graaf. Defendant Frank Caraballo is represented by Mark A. Kaplan, Esq. and Natasha Sen, Esq.

Defendant is charged in a four count Second Superseding Indictment as follows: Count one: conspiring to distribute mixtures or substances containing detectable amount cocaine, cocaine base, and heroin, as part of a conspiracy involving 280 grams or more of a mixture or substance containing a detectable amount of cocaine base, in violation of 21 U.S.C. §§ 841(a), (b)(1)(A), 846; Count two: possession and use of a firearm in furtherance of a drug trafficking crime with an allegation that Defendant discharged the firearm and caused the death of Melissa Barratt by murder, in violation of 18 U.S.C. §§

924(c)(1)(A)(iii), (j)(1); Count three: possession of a firearm in furtherance of a drug trafficking crime, in violation of 18 U.S.C. § 924(c)(1)(A); and Count Four: possession of a firearm by a felon, with an allegation that Defendant has been convicted of four prior drug trafficking felonies in violation of 18 U.S.C. §§ 922(g)(1), 924(a)(2), (e)(1).

## **I. FINDINGS OF FACT.**

### **A. The Barratt Homicide Investigation.**

At approximately 10:45 a.m. on the morning of July 29, 2011, law enforcement responded to a report that a body of a woman had been found in a wooded area down an embankment near a stream approximately thirty yards from the East West Road in Dummerston, Vermont. The location was “off the beaten path,” Tr. 6/14/13 (“Tr.”) at 144, and on the outskirts of the town limits of Brattleboro, Vermont. When law enforcement arrived on the scene, they found the woman on the ground in a kneeling position with her hands clasped in front of her. She had a gunshot wound to the back of her head and because of the position of her body, her clasped hands, and the absence of a firearm nearby, law enforcement concluded that the woman did not commit suicide. It also did not appear that her body had been carried to the location at which it was found as there was no trail of blood or other signs that would support that conclusion. Law enforcement suspected that the woman was the victim of a homicide and that her assailant could still be armed. Based upon information from a construction crew that was working approximately a half mile from the scene and who reported they had heard what sounded like a gunshot that morning, law enforcement concluded the apparent homicide had occurred that day.

By the tattoos on the body of the deceased, criminal activity records, and a previous photo, law enforcement identified the woman as Melissa Barratt. Law enforcement learned that Ms. Barratt had been arrested on May 31, 2011 in Brattleboro, in conjunction with the sale of narcotics. After her arrest, law enforcement interviewed Ms. Barratt, who advised that she was involved in drug activity in Brattleboro with an individual named Frank Caraballo, that “she was extremely nervous and afraid of a Frank

Caraballo,” and that “if he knew that she was talking to [the police officer], he would hurt her, kill her.” Tr. at 18-19. Ms. Barratt also told law enforcement that Defendant had “access to guns and was armed and [she] was afraid of him.” Tr. at 38. These firearms included “shotguns, Tech 9[]s and other types of weapons.” Tr. at 194-95. Ms. Barratt described Defendant as someone who was “very dangerous” and told law enforcement that “she had firsthand knowledge of him doing or assaulting or possibly involved in other homicides.” Tr. at 148. She “did not want to give out any information about him because of her fear of him. And the fact that if she did provide information she would basically be killed.” *Id.* Law enforcement had information that Ms. Barratt was still associated with Defendant on the day of the homicide.

In the late morning of July 29, 2011, Detective Sergeant Richard Holden of the Vermont State Police (“VSP”) reviewed the radio log for the Barratt homicide investigation. At the time, he was employed in VSP’s Bureau of Criminal Investigation, which handled all major crimes for the VSP including homicides, missing persons, thefts, rapes, and kidnappings. He contacted VSP Detective Frank LaBombard, the case agent for the Barratt homicide investigation, to see if he needed any help. Detective LaBombard showed Detective Sergeant Holden digital photos of Ms. Barratt’s deceased body that appeared to confirm that Ms. Barratt was the victim of a homicide. Indeed, it was Detective Sergeant Holden’s belief at the time that the Barratt homicide was “a coldblooded execution.” Tr. at 26.

A command post for the Barratt homicide investigation was set up at the West Dummerston Fire Department approximately one half mile from the crime scene and approximately fifteen minutes from the Brattleboro area. Law enforcement gathered at the command post to assign tasks and to ensure that information gleaned from the investigation was shared with appropriate personnel. Throughout the day, information that was obtained was disseminated from the command post to law enforcement officers working on the case in the field. Detective Sergeant Holden was tasked with obtaining information regarding Defendant. He was informed that Brattleboro law enforcement

had engaged in at least three recent controlled buys of narcotics from Defendant for which he had not yet been arrested or charged.

Detective Sergeant Holden contacted VSP's Fusion Center which, at the time, served as an intelligence center and database for law enforcement. Through the Fusion Center, Detective Sergeant Holden determined that the Fusion Center had processed a request for information regarding Defendant one month previously which was "extremely important" to him because it indicated "something was going on which is very valuable to us." Tr. at 46. Detective Sergeant Holden discovered Defendant's criminal history included drug activity. He also determined that Defendant's brother was Michael Caraballo who had been charged a few months prior to the Barratt homicide with a drive-by shooting in southern Vermont. Detective Sergeant Holden read the police reports in Michael Caraballo's case, but he did not have any personal knowledge of that investigation or prosecution other than it was his understanding that Frank and Michael Caraballo had worked together in selling illegal drugs in the Brattleboro area. Detective Sergeant Holden found the information regarding Michael Caraballo's drive-by shooting case concerning because it suggested that Defendant may have access to firearms through his brother. Based upon this information, Detective Sergeant Holden considered Defendant an immediate danger to law enforcement, noting that: "He's armed and dealing drugs. I'm pretty sure that's a threat to law enforcement." Tr. at 47. Detective LaBombard echoed these concerns. He testified that law enforcement's arrest of Michael Caraballo included gun possession charges and that when Michael "went to jail . . . Frank had taken over the operation and was distributing narcotics in the area" and that some of Defendant's background included "criminal involvements with assaults." Tr. at 150.

After it became clear that Defendant was "a person of interest" in the Barratt homicide investigation, Detective Sergeant Holden "thought it was extremely important to locate [Defendant] that day just because of the safety aspects of it." Tr. at 25. Detective Sergeant Holden described those safety concerns as follows:

I was concerned that if there was information leaked before the homicide occurred we did not know what extent that information was. We knew that we had our narcotics officers in deep working with their C.I.s [confidential informants] investigating Frank Caraballo. And we were concerned that if there was some sort of information leaked we weren't sure if he was going to be going after any sort of C.I.s or narcotic officers at that point.

We were also concerned that if [Frank Caraballo] was stopped by a local law enforcement officer who did not know the situation of what was ongoing that he would be at risk or she would be at risk at the time of the car stop . . . [because] there wasn't a gun found at the scene, I mean we had to assume, you know, the person was still armed and dangerous. If a local police officer stopped the vehicle for, you know, a minor infraction such as speeding and they had no idea what was going on just the totality of the stress of the driver, you know, there could have been a shoot out in a public area. We just didn't know. That was another concern of ours. . . . [Mr. Caraballo] wouldn't know why he was being stopped. I would have to assume that he was thinking it was in connection with the homicide, but that's not necessarily the case.

Tr. at 26-27. Detective Sergeant Holden's safety concerns extended to people "involved in the drug operation" with Defendant. Tr. at 27. He was aware that, in addition to Ms. Barratt, Defendant was involved with "a lot of other individuals in the Brattleboro area. And we weren't sure why the homicide occurred. And we were concerned at that point about the safety of the other people." Tr. at 27-28.

Law enforcement was also concerned about the possible destruction or dissipation of evidence. Detective LaBombard credibly testified that in the Barratt homicide investigation, access to the potential assailant shortly after the homicide was likely to yield important and irreplaceable evidence such as a homicide weapon, gunshot residue, DNA, clothing, blood splatters on clothing or shoes, and footprint and tire impressions that could be tied to the crime scene if discovered promptly, but which may be destroyed, dissipate, or disappear thereafter if the assailant was not promptly apprehended.

Law enforcement personnel conferred to consider their options. They considered having confidential informants contact Defendant, discern his whereabouts, and arrange a

meeting. They also considered having VSP troopers posted on major roadways in the hope of identifying Defendant's passing vehicle based upon their knowledge of the vehicles that had been associated with him. Law enforcement was aware that Defendant had no apparent permanent residence in Vermont but, instead, stayed in hotels and travelled frequently to and from Massachusetts where his family resided.

**B. The Decision to "Ping" Defendant's Cellphones.**

Law enforcement also considered the possibility of obtaining a search warrant for Defendant's cell phones. Through controlled buys with Defendant, law enforcement was aware that Defendant had recently used two cell phone numbers: (413) 657-3540 and (802) 288-6558. Detective Sergeant Holden determined that the time necessary to obtain a warrant would be approximately six hours based upon his prior experience. Law enforcement would then need to serve the warrant on the cell phone companies and await a response which, in his experience, would not be immediate in the absence of exigent circumstances but instead was likely to involve "a huge delay of getting the information from the company that we're requesting it from." Tr. at 28. Detective Sergeant Holden concluded that there were sufficient safety concerns to justify a request for cell phone data without a warrant. At the time, it was his understanding that applicable law permitted law enforcement to request a warrantless search of cell phone location information if there was an emergency involving a threat of serious bodily injury or death.<sup>1</sup> This investigative technique, commonly referred to as cell phone "pinging," consists of the cell phone carrier surreptitiously accessing by satellite the cell phone's GPS location, or if unavailable, its location in terms of its proximity to the nearest cell phone tower. At the time of the Barratt homicide investigation, Detective Sergeant

---

<sup>1</sup> 18 U.S.C. § 2702(c)(4) authorizes cell phone carriers to provide "a record or other information pertaining to a subscriber to or customer of [cell phone] service . . . to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency."

Holden had obtained such information without a warrant on two previous occasions: one involving a kidnapping and the other involving a missing person.

Detective Sergeant Holden conferred with Detective LaBombard and credibly testified that they were “both of the mindset like this is, this is a legitimate emergency. We have to do this or potentially someone is going to get hurt or killed.” Tr. at 29. He also consulted with Windham County State’s Attorney, Tracy Shriver, who was at the command center and who agreed “that the cell phone pinging at that time was the way to go” and “was appropriate and it was probably the best action to take.” Tr. at 30-31. The court finds that, in deciding to ping Defendant’s cell phones, law enforcement held a good faith, reasonable belief that there was a serious and imminent threat to human life and that federal law authorized a warrantless cell phone pinging in those circumstances.

Thereafter, Detective Sergeant Holden contacted the Fusion Center to assist in pinging Defendant’s cell phones. He spoke with VSP Detective Cari Crick, briefed her on the situation, and advised her that he had the state’s attorney’s approval to proceed with a warrantless request to ping Defendant’s cell phones and that it was an emergency. Detective Crick had some familiarity with the Barratt homicide investigation as she had assisted Detective Sergeant Holden with his requests that day for information regarding Frank Caraballo. After consulting with Detective Sergeant Holden, Detective Crick contacted Sprint Nextel and explained the situation and the information she was requesting. Sprint Nextel made the determination to fax Detective Crick a request form consisting of a one-page document titled “Mandatory Information for Exigent Circumstances Requests.” Gov’t Ex. 1. The form requires that Sprint Corporate Security be called before the request form is faxed and that any such fax be accompanied by an agency cover sheet. The form also requires identification of the law enforcement agency requesting the information, its address, phone number, and fax number, as well as the requesting agent’s name, title, email address, and his or her supervisor’s name and phone number.

In completing the form, Detective Crick requested “Precision Location of mobile device (GPS Location)” for both of Defendant’s cell phones, as well as subscriber information and call detail records with cell site information (within the past week). The form requires the requesting agent to certify that he or she has been granted authority by the identified law enforcement agency “to determine and declare an exigent situation involving . . . [an] immediate danger of death or serious bodily injury to any person[.]” *Id.* Detective Crick’s notes, created at the time, reflect her understanding that the state’s attorney had requested the ping and include the phrase “primary suspect” after noting that the request was for Frank Caraballo’s cell phone. Tr. at 125; Gov’t Ex. 7. At the bottom of the form, Detective Crick certified that she had the authority to declare an exigent situation which she described as “Male with phones is suspect in possible homicide.” Gov’t Ex. 1.<sup>2</sup> Detective Crick further certified on the form under penalty of perjury that the information she had provided was true and correct.

Detective Crick credibly testified that, when she completed the Sprint Nextel pinging request form, she believed applicable law permitted a warrantless pinging of a cell phone where there was “some sort of emergent incident occurring that there was a threat to an individual or somebody else” that created a “safety issue of concern.” Tr. at 115. She relied upon “the immediate danger of death or serious bodily injury to . . . any person,” Tr. at 124, provision of the request form. Detective Crick believed these circumstances existed in the Barratt homicide investigation based upon what Detective Sergeant Holden had told her. The court finds that she held a good faith belief that an exigent situation existed and that applicable law authorized a warrantless cell phone pinging on that basis.

---

<sup>2</sup> Detective Crick tried to “hit the highlights of the request, not the specifics,” Tr. at 125, and she did not include all of the information she had at the time regarding the Barratt homicide investigation.



**C. The Technology of Defendant's Nextel Phone and Sprint Nextel's Terms and Conditions of Services with Regard to It.**

A Sprint Nextel cell phone acts as a cordless handset that connects with a cell tower or antenna in order to transmit data and call information. Each cell phone tower is connected to what is called a "switch" which is part of the public telephone network which transmits and receives domestic and international calls. When a Sprint Nextel cell phone is on, it is in communication with cell phone towers, even when a call is not being made. Through its communication with the cell tower, the cell phone is constantly updating the system with its location, asking, in effect, "Do you have any calls for me?" Tr. at 73-74. This process is necessary because the cell tower, in turn, needs to know the approximate location of the cell phone so that it may send calls to that location. The cell phone's communication with the cell tower does not occur on the same channel that it uses to make phone calls but, instead, uses a "control channel." There is no notification to the cell phone user that this communication is taking place and the cell phone user has no control or involvement in these communications other than placing the phone in "on" mode. If the cell phone is in "off" mode, no communications take place.

Sprint Nextel's technology for responding to emergency requests for cell phone location information varies depending upon the type of cell phone involved. A Sprint cell phone uses a technology called CDMA. A Nextel cell phone uses a network technology called GSM. The two types of technology differ only in the manner in which the data is connected. Both types of technology attempt to use GPS satellites to determine the cell phone's location. The majority of cell phones sold by Sprint Nextel in 2011 contained a GPS receiver which permits access to satellite information in order to provide enhanced location services when the user accesses 911. The GPS receiver, if activated, also provides information to Sprint Nextel regarding the cell phone's location. If the cell phone is turned off, no GPS information is transmitted.

Defendant's Nextel (802) 288-6558 cell phone is the type of phone that attempts to use three or more GPS satellites to obtain location information to calculate its location

by longitude and latitude. If the cell phone is unable to locate three or more satellites, it will automatically “step down” to determine what cell phone tower the phone is “hitting off of,” Tr. at 82, which it will use to provide a location for the phone within a default 4,999 meter radius. This same default radius will be provided whether the cell tower is ten feet away or five miles away because, in this instance, the location data merely reveals the cell tower with which the cell phone is communicating.

In 2011, Sprint Nextel offered two types of cell phone service: a “postpaid” service that involves the cell phone service subscriber receiving a monthly bill in the mail for his or her usage and a “prepaid” service which means the subscriber purchases minutes in advance and when those minutes have been used, the subscriber loses the ability to make phone calls until additional minutes are purchased. Defendant’s Nextel phone used a prepaid plan. It was registered to “Walter Smith,” which could be information Defendant provided to Sprint Nextel or could be a default name used by the Sprint Nextel representative who sold Defendant the phone. When a cell phone is on a prepaid plan, Sprint Nextel does not need to know the identity of the account holder. When a cell phone is not prepaid, Sprint Nextel requires a credit check so that it can verify the identity of the account holder. Otherwise, the two types of cell phone plans are identical.

Sprint Nextel’s general terms and conditions of service are provided to customers in conjunction with the purchase and sale of a Sprint Nextel cell phone. By activating the cell phone, the cell phone subscriber is deemed by Sprint Nextel to have agreed to those general terms and conditions. If the purchase and sale transaction occurs online or over the phone, the subscriber is required to acknowledge that he or she accepts Sprint Nextel’s general terms and conditions.

In 2011, Sprint Nextel’s general terms and conditions of service advised its customers, in relevant part that: “Our networks generally know the location of your Device when it is outdoors and/or turned on. By using various technologies to locate your Device, we can provide enhanced emergency 911 services and optional location-

enabled services provided by us or a third party.” Govt’s Ex. 2 at 13. Sprint Nextel’s privacy policies, which are incorporated by reference in its general terms and conditions of service, describe how Sprint Nextel collects, accesses, uses, and discloses its customers’ personal information in providing “Services” which are defined as all “products, services, and web sites.” Gov’t Ex. 3 at 1. In relevant part, they advise:

We collect personal information about you in various ways. We may also get information from other sources and may combine it with information we collect about you.

Information you give us. The personal information we collect includes information you give us such as name, postal address, telephone number, e-mail address, date of birth, social security number or other government identification number, demographics, activities, **location information**, and personal preferences. You may give us information in a variety of ways such as when you sign up for Services, communicate with customer care or register on sprint.com. Personal information does not include information that is not used to identify you including aggregate or anonymous information.

Information that we automatically collect. **We automatically receive certain types of information whenever you use our Services. We may collect information about your device, your computer, and online activities.** For example, we collect your device’s and computer’s IP address, the date and time of your access and the type of browser you use. We also collect information about your device’s and computer’s operation system, **your location**, and the Web site from which you came and then went and Web sites you visit on your device. We may link information we automatically collect with personal information, such as information you give us at registration or check out.

Information we collect when we provide Services includes when your wireless device is turned on, how your device is functioning, device signal strength, **where it is located**, what device you are using, what you have purchased with your device, how you are using it, and what sites you visit.

We may use systems or tools to follow your use of our Services, including using cookies, web beacons and other tracking mechanisms.

\* \* \*

*Id.* (emphasis supplied).

Sprint Nextel's privacy policies further advise customers that the company will use the customer's personal information "to do things like: . . . [r]espond to legal process and emergencies." *Id.* at 1-2. They advise that Sprint Nextel does not share personal information with third parties other than in certain identified instances which include, under the title "Protection of Sprint Nextel and Others," a disclosure that: "We may access, monitor, use or disclose your personal information or communications to do things like: . . . comply with the law or respond to lawful requests or legal process . . . [and] respond to emergencies[.]" *Id.* at 2.

In 2011, Sprint Nextel's practice was to provide to law enforcement cell phone data without a warrant if there was a good faith certification that there were exigent circumstances consisting of an immediate risk of either death or serious bodily injury. Sprint Nextel believed this practice was authorized by 18 U.S.C. § 2702(c) because its legal counsel reviewed the Sprint Nextel request form and Sprint Nextel's protocols for compliance with federal law and concluded that they were in compliance.

At the time of the Barratt homicide, Sprint Nextel annually processed several thousands of exigent circumstances requests. In doing so, it did not conduct its own determination of exigent circumstances because: "Essentially we don't want an analyst to override law enforcement in the field. They know better the situation of what's going on, they may have some sensitive information that they have not shared. They have just given us a general description of the exigen[cy] and, therefore, we don't want somebody sitting in our office to, you know, second guess them when we don't actually know . . . what's actually going on." Tr. at 107-08. Instead, it is and was Sprint Nextel's practice and policy to rely on law enforcement certification under oath subject to the penalties of perjury that the information provided on Sprint Nextel's "Mandatory Information for Exigent Circumstances Requests" is true and accurate. The court finds that Sprint Nextel acted in good faith and based upon a good faith and reasonable

understanding of applicable law in developing and implementing its pinging policies and practices.

**D. How Sprint Nextel Pings a Cell Phone.**

When Sprint Nextel pings a cell phone, it uses a tool on its computer that permits it to insert a cell phone number, click a button, and initiate a request through its network to the cell phone to identify its GPS coordinates. This communication takes place through the control channel and can only occur in areas where Sprint Nextel has network access. The cell phone responds by producing its location information to Sprint Nextel's surveillance analyst. The analyst then relays that location data to law enforcement. The person who owns or possesses the pinged cell phone typically receives no signal or other communication that the pinging has occurred. If the pinging process fails, the analyst is still able to determine the location of the cell tower with which the cell phone is communicating as that process takes place automatically and continuously if the cell phone is on. The pinging process occurs in the same manner regardless of whether the cell phone is on a prepaid or postpaid plan. Cell phone pinging is more likely to be successful and more accurate when the pinged cell phone is not in a building because the cell phone needs access to GPS satellites in order to "get the good GPS ping." Tr. at 109. If it cannot, it will default to the 4,999 meter cell phone tower radius.

Law enforcement must call Sprint Nextel to initiate each separate ping unless a secure network has been established, which was not the case here. When initiating a ping, there is no means to determine whether the cell phone is in a public or private location. The only information that is transmitted pursuant to a ping is either the GPS location determined by satellites or the location within a 4,999 meter radius of the nearest cell phone tower. The contents of calls are not divulged.

In addition to pinging information, an exigent circumstances request may ask for subscriber information, which includes the name and address of the subscriber. It may also seek call detail records with cell site information within the past week which identifies the phone numbers called, the time the calls began and ended, and the cell

tower sites that were used when the calls ended. Again, the contents of cell phone calls are not disclosed.

**E. The Pinging of Defendant's Cell Phones.**

At approximately 3:15 p.m. on July 29, 2011, Detective Crick asked Sprint Nextel to ping both of the cell phones associated with Defendant. Sprint Nextel faxed to her the exigent circumstances request form which she completed and faxed back at approximately 3:20 p.m. The first pinging took place at 3:43 p.m. for Defendant's (413) 657-3540 cell phone. These pings failed and revealed no information. Thereafter, law enforcement requested a ping on Defendant's (802) 288-6588 Nextel cell phone. This ping worked at 4:03 p.m. and revealed that Defendant's 6588 cell phone was in the Brattleboro area. Through a series of pings, between approximately 4:03 p.m. and 5:20 p.m. (thirteen successful pings within approximately an hour and ten minutes), law enforcement determined that Defendant's 6558 cell phone was being transported north on Interstate 91 and had reached Springfield, Vermont. Of the thirteen pings, four provided only cell tower information. As Detective Crick received the information, she used Google Maps to further identify the 6558 cell phone's location and relayed this information to law enforcement in the field.

With the final series of pings, Detective Crick determined that Defendant was in Springfield's town center, and she notified local law enforcement agencies of Defendant's probable location. Through surveillance and information received regarding the two vehicles associated with Defendant, local law enforcement identified Defendant's vehicle at a McDonald's in Springfield's town center. The two final pings at 5:11 p.m. and 5:20 p.m. assisted in confirming this location. At this point, law enforcement decided to cease pinging and to issue a "Be on the Lookout," which was disseminated throughout the State of Vermont. Law enforcement also positioned personnel on major access routes to Massachusetts, which were identified as Interstate 91 and Route 5. Through visual surveillance, they determined that Defendant's vehicle had left the McDonald's and was travelling on Route 10 towards Chester and Ludlow, Vermont.

Law enforcement personnel planned to maintain surveillance of Defendant's vehicle while they discussed whether to effect a stop. It was ultimately determined that there was probable cause to arrest Defendant for the controlled buys and to stop his vehicle on this basis. At the time, law enforcement believed that there was insufficient evidence to arrest Defendant for the Barratt homicide.

When a law enforcement officer visually confirmed that Defendant was in the target vehicle, he conducted a stop of the vehicle, and arrested Defendant on drug charges. Although some law enforcement reports describe the basis for the arrest as "unrelated drug charges," Detective Sergeant Holden disagrees with this characterization and asserts that Defendant was stopped and arrested on drug charges (which may have been related) only because there was not enough information to arrest him in connection with Ms. Barratt's apparent homicide. It was the latter crime, however, that gave rise to law enforcement's surveillance activities on July 29, 2011.

Evidence was located in Defendant's vehicle which the Government intends to offer at trial, including Defendant's 6558 cell phone. After his arrest, Defendant was transported to a VSP barracks where he was interviewed. After receiving *Miranda* warnings, Defendant made a number of statements which the government characterizes as "false exculpatory statements about when he last saw Barratt" (Doc. 48 at 8) which it seeks to offer at trial.

## **II. CONCLUSIONS OF LAW AND ANALYSIS.**

### **A. Standard of Review.**

Defendant seeks suppression of "all of the evidence recovered in the vehicle in which he was travelling, all of the evidence found on him, and all of the statements he made to police officers after they stopped his vehicle and arrested him on July 29, 2011." (Doc. 38 at 1.) He claims suppression is warranted because "[t]he government violated [his] Fourth Amendment rights by using his cellular telephone . . . to electronically track

him without a warrant.” *Id.*<sup>3</sup> The Government opposes the motion, contending that no “search” occurred within the Fourth Amendment and that, even if a search occurred, it was reasonable for purposes of the Fourth Amendment because of the exigent circumstances, the automobile exception, good faith reliance upon applicable law, and because Defendant’s location would have inevitably been discovered.

“It is well established that the burden of production and persuasion generally rest upon the movant in a suppression hearing.” *United States v. Arboleda*, 633 F.2d 985, 989 (2d Cir. 1980) (internal quotation marks omitted). “The movant can shift the burden of persuasion to the Government and require it to justify its search, however, when the search was conducted without a warrant.” *Id.* at 989. “[T]he controlling burden of proof at suppression hearings should impose no greater burden than proof by a preponderance of the evidence.” *United States v. Matlock*, 415 U.S. 164, 177 n.14 (1974).

**B. Whether Gathering Real-Time Location Data From Defendant’s Cell Phone was a “Search” in the Circumstances of this Case.**

**1. *Jones* and the Supreme Court’s Surveillance Jurisprudence.**

In analyzing Defendant’s request for suppression, the court must first determine whether the pinging of Defendant’s cell phone constituted a “search” under the Fourth Amendment. In *United States v. Jones*, 132 S. Ct. 945 (2012), the Supreme Court concluded that the government’s physical placement of a GPS device on the undercarriage of the defendant’s motor vehicle was a physical occupation of private property for the purpose of obtaining information and thus a “search” within the Fourth Amendment. *Jones*, 132 S. Ct. at 949. The parties here agree that no physical

---

<sup>3</sup> Defendant argues that Sprint Nextel was acting as an agent of the government when it provided, at the government’s request, the real-time location data for Defendant’s cell phone. (Doc. 38 at 9-10.) The government does not contest Defendant’s agency argument. Under *Skinner v. Ry. Labor Exec. Ass’n*, 489 U.S. 602, 614 (1989), “the [Fourth] Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government.” *Id.* “Although a wholly private search falls outside the scope of the Fourth Amendment, a search conducted by private individuals at the instigation of a government officer or authority constitutes a governmental search for purposes of the Fourth Amendment.” *Cassidy v. Chertoff*, 471 F.3d 67, 74 (2d Cir. 2006) (internal citations omitted).



occupation or trespass took place in the pinging of Defendant's cell phone and that this case is thus governed not by *Jones* but by *Katz v. United States*, 389 U.S. 347 (1967), which *Jones* left intact. *See Jones*, 132 S. Ct. at 953 (observing that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis"). *Jones* nonetheless provides useful guidance as to the state of the law when cell phone data is used to track an individual's movements or identify his or her location.

The *Jones* majority observed that "[t]his Court has to date not deviated from the understanding that mere visual observation does not constitute a search" and that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* (internal quotation marks omitted). The majority nonetheless acknowledged that "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy," *id.* at 954, although it did not reach that question. None of the justices in *Jones* affirmatively concluded that a "search" consists of short-term location monitoring of a vehicle's location on a public highway through a GPS device. However, that possibility remains an open question after *Jones* because the Supreme Court is divided regarding how this issue should be analyzed.

In his *Jones* concurrence, Justice Alito would have "analyze[d] the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." *Id.* at 958 (Alito, *J.*, concurring). In highlighting that "the [Fourth] Amendment should be understood as prohibiting every unjustifiable intrusion by the government upon the privacy of the individual," *id.* at 959 (internal quotation marks omitted), Justice Alito argued that the majority's opinion "largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation)." *Id.* at 961

(Alito, *J.*, concurring). Justice Alito further opined that the majority’s “reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked.” *Id.* at 962 (Alito, *J.*, concurring). His concurrence focused on the fact that law enforcement used the GPS to track “every movement” the defendant made in the vehicle he was driving for over four weeks. In contrast, he observed that “relatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable.” *Id.* at 964 (Alito, *J.*, concurring). The majority opinion took issue with this conclusion, observing:

The concurrence posits that “relatively short-term monitoring of a person’s movements on public streets” is okay, but that “the use of longer term GPS monitoring in investigations of *most offenses*” is no good. That introduces yet another novelty into our jurisprudence. There is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated. And even accepting that novelty, it remains unexplained why a 4-week investigation is “surely” too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an “extraordinary offens[e]” which may permit longer observation. What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist? We may have to grapple with these “vexing problems” in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.

*Jones*, 132 S. Ct. at 954 (internal citations omitted). Justice Sotomayor, in her concurring opinion, also expressed concern about the constitutionality of short-term GPS location monitoring:

In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain

abusive law enforcement practices: “limited police resources and community hostility.”

*Jones*, 132 S. Ct. at 955-56 (Sotomayor, *J.*, concurring) (internal citations omitted).

*Jones* thus stands for the proposition that while the Court has not affirmatively concluded that a “search” occurs for purposes of the Fourth Amendment whenever there is government initiated short-term GPS monitoring of a vehicle’s whereabouts on a public highway through an individual’s cell phone, it remains an open question to be decided under *Katz*.

In *Katz*, the Supreme Court held that “the Fourth Amendment protects people, not places,” *Katz*, 389 U.S. at 351, and that “once it is recognized that the Fourth Amendment protects people—and not simply ‘areas’—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.” *Id.* at 353. In his concurring opinion in *Katz*, Justice Harlan delineated a two-part test for determining when an intrusion is unreasonable, which the Supreme Court has subsequently adopted and applied. *See Jones*, 132 S. Ct. at 950. “[F]irst, . . . a person [must] have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’” *Katz*, 389 U.S. at 361 (Harlan, *J.*, concurring). The Supreme Court has described *Katz* as the “lodestar” for “determining whether a particular form of government-initiated electronic surveillance is a ‘search’ within the meaning of the Fourth Amendment.” *Smith v. Maryland*, 442 U.S. 735, 739-41 (1979); *see also United States v. Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008) (“A defendant seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment must show that he had a ‘legitimate expectation of privacy’ in the place searched. This inquiry involves two distinct questions: first, whether the individual had a subjective expectation of privacy; and second, whether that expectation of privacy is one that society accepts as reasonable.”).

The government argues that because all of the cell phone pinging in this case took place while Defendant was in a motor vehicle on a public highway, he cannot be said to have a subjective expectation of privacy because his location was in fact public. The problem with this argument is twofold. First, it is undisputed that the information in question would have been transmitted to law enforcement via the pinging regardless of whether Defendant was in the sanctity of his home or on a public highway. Thus, unlike a beeper placed on a motor vehicle, Defendant's location was not derived in any respect *because* he was in a motor vehicle and thus had voluntarily exposed his location to the public. Second, because law enforcement did not know Defendant's actual location or path of travel, there was no means of tracking Defendant's movements using traditional surveillance methods and publicly available technology. Instead, Defendant's location was obtained *solely* through the use of nonpublic technology that would have revealed his likely presence in his own home even if that fact was not evident from visual surveillance. See *Kyllo v. United States*, 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."). The Supreme Court's electronic surveillance jurisprudence explains why these facts are important.

In *United States v. Knotts*, 460 U.S. 276 (1983), the Court addressed the warrantless use of a "beeper" to assist in law enforcement surveillance of a suspect's activities. In that case, a private business consented to law enforcement's installation of a beeper inside a five-gallon container of chloroform intended for sale to certain suspects. When one of the suspects purchased the item, officers followed his car to a cabin. At one point, the suspect eluded the officers, but the officers were able to relocate him based upon the signal from the beeper. The Court addressed whether this electronic monitoring through the use of the beeper "invade[d] any legitimate expectation of privacy," and concluded it did not. *Id.* at 279-80, 285. In doing so, the Court noted that the surveillance "amounted principally to the following of an automobile on public streets

and highways” and that there is a “diminished expectation of privacy in an automobile.”

*Id.* at 281. It held that:

A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

*Id.* at 281-82.

The Court recognized that the owner of the cabin, which was the vehicle’s final destination, “had the traditional expectation of privacy within a dwelling place insofar as the cabin was concerned,” but “no such expectation of privacy extended to the visual observation of [the] automobile arriving on [the] premises after leaving a public highway.” *Id.* at 282; *see also id.* at 285 (noting officer could have visually surveilled car leaving public highway and arriving at cabin). The Court concluded:

“[T]he fact that the officers in this case relied not only on visual surveillance, but on the use of the beeper to signal the presence of [the] automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case. . . . Insofar as [the defendant’s] complaint appears to be simply that scientific devices such as the beeper enabled the police to be more effective in detecting crime, it simply has no constitutional foundation. We have never equated police efficiency with unconstitutionality, and we decline to do so now.”

*Id.* at 282, 284. The Court observed that there was “no indication that the beeper was used in any way to reveal information . . . within the cabin, or in any that would not have been visible to the naked eye from outside the cabin.” *Id.* at 285.

One year after its decision in *Knotts*, the Court again turned to the use of a beeper in *United States v. Karo*, 468 U.S. 705 (1984). There, the Court addressed issues “unresolved” in *Knotts*, including “whether monitoring of a beeper falls within the ambit

of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance.” *Id.* at 707. In *Karo*, government agents placed a beeper in a can of ether that was later sold to the defendants. The agents used the beeper to trace the can of ether as it moved to and from several locations and to its final location inside a house in Taos, New Mexico. *Id.* at 708-10. The agents then used the beeper to confirm that the can of ether remained in the house. *Id.* The Court concluded that “the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.” *Id.* at 714. The Court explained:

In this case, had a DEA agent thought it useful to enter the Taos residence to verify that the ether was actually in the house and had he done so surreptitiously and without a warrant, there is little doubt that he would have engaged in an unreasonable search within the meaning of the Fourth Amendment. For purposes of the Amendment, the result is the same where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house. The beeper tells the agent that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched. Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers’ observations but also establishes that the article remains on the premises. Here, for example, the beeper was monitored for a significant period after the arrival of the ether in Taos and before the application for a warrant to search.

*Id.* at 715.<sup>4</sup> As applied to this case, *Knotts* and *Karo* pose more questions than they answer. On the one hand, at all times during the pinging process, Defendant was on a

---

<sup>4</sup> In *Karo*, the government had argued that a holding opposite of *Knotts* would lead to anomalous results: “If agents are required to obtain warrants prior to monitoring a beeper when it has been withdrawn from public view, the Government argues, for all practical purposes they will be forced to obtain warrants in every case in which they seek to use a beeper, because they have no way of knowing in advance whether the beeper will be transmitting its signals from inside private premises.” *Id.* at 718. The Court observed this was not a compelling argument, and further noted it was “not a particularly attractive case in which to argue that it is impractical to

public highway and his location thus *could have been* observed by law enforcement and the public. On the other hand, Defendant's location was discovered only after law enforcement surreptitiously used technology that was not generally available to the public and which would have revealed Defendant's presence in his own home even if that information could not have been gleaned through visual surveillance. A Fourth Amendment analysis entirely dependent upon the fortuity of a criminal defendant entering his or her own home during the pinging process is likely to prove as unworkable as the definition of "short term" GPS location monitoring Justice Alito deemed presumptively reasonable in *Jones*. See *State v. Earls*, 2013 WL 3744221, at \*12 (N.J. July 18, 2013) (holding cell phone user had a reasonable expectation of privacy in cell phone location information under state constitution and noting: "Modern cell phones also blur the historical distinction between public and private areas because cell phones emit signals from both places. In this case, defendant was located in a motel room, not on a public highway. Yet law enforcement had no way of knowing in advance whether defendant's cell phone was being monitored in a public or private place.").

## **2. Cell Phone Location Data Jurisprudence.**

The parties agree that only one circuit court, the Sixth Circuit, has thus far addressed the use of real-time location data to track a cell phone user. In *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), the Sixth Circuit concluded that there was no Fourth Amendment violation because the defendant "did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone." *Id.* at 777. In that case, law enforcement obtained an order from a federal magistrate judge, authorizing the release of, among other things, GPS real-time location data and cell phone ping data in order to determine a drug courier's location while he was en route to deliver drugs. The Sixth Circuit found prior authorization important, but not dispositive. *Id.* at 779 ("Although not necessary to find that there was no Fourth

---

obtain a warrant, since a warrant was in fact obtained in this case, seemingly on probable cause." *Id.*

Amendment violation in this case, the Government's agreement is strengthened by the fact that the authorities sought court orders to obtain information on Skinner's location from the GPS capabilities of his cell phone."). Instead, the court focused on the fact that the cell phone technology was "voluntarily procured," *id.* at 777, and used on a public highway. *Id.* at 781 ("Because authorities tracked a known number that was voluntarily used while traveling on public thoroughfares, [the defendant] did not have a reasonable expectation of privacy in the GPS data and location of his cell phone."). The court found it irrelevant that law enforcement obtained the defendant's location exclusively through non-public technology, reasoning: "There is no inherent constitutional difference between trailing a defendant and tracking him via technology. Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system." *Id.* at 778. The *Skinner* court did not explain why a pay-as-you-go phone should be treated differently from any other type of cell phone although it emphasized that this type of phone is popular with drug couriers, "and thus presumably more difficult to trace." *Id.* at 774.

### **3. The Voluntary Disclosure Doctrine.**

Defendant argues that *Skinner* was wrongly decided for a number of reasons, including its assumption that, if a cell phone is "voluntarily procured," all expectations of privacy with regard to location data information are presumptively waived. The court agrees that the proper focus is on voluntary disclosure, not voluntary procurement, and that it should not matter under the Fourth Amendment whether a cell phone is prepaid or postpaid as that fact has nothing to do with the user's expectations of privacy.

Defendant relies on *Smith v. Maryland*, 442 U.S. 735 (1979) for the distinction between voluntarily conveying information, for which one has no expectation of privacy, and automatic transmission of information, which Defendant argues a reasonable person would expect to be kept private. In *Smith*, the government installed at the telephone company's headquarters a "pen register" that recorded the numbers dialed on a certain telephone; the pen register, however, did not record the content of the phone calls. *Id.* at



736 n.1, 737, 741. The Court concluded there was no legitimate expectation of privacy in the numbers the defendant dialed, reasoning: “First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.” *Id.* at 742. “Second, even if [the defendant] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable. This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Id.* at 743-44 (internal quotation marks and citations omitted).

The *Smith* Court analogized the facts in the case before it to the facts in *United States v. Miller*, 425 U.S. 435 (1976), wherein the Court held that “a bank depositor has no ‘legitimate expectation of privacy’ in financial information ‘voluntarily conveyed to banks and exposed to their employees in the ordinary course of business.’” *Id.* at 443. The Court explained “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.” *Id.* The *Smith* Court concluded that *Miller*’s analysis “dictate[d]” the result in *Smith*: “When he used his phone, [the defendant] voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business. In so doing, [the defendant] assumed the risk that the company would reveal to police the numbers he dialed.” *Smith*, 442 U.S. at 744.

In determining whether a defendant *voluntarily conveys* location data through the use of a cell phone, courts have taken divergent approaches.<sup>5</sup> The Second Circuit has not

---

<sup>5</sup> Compare *In re: Application of the United States of America for Historical Cell Site Data*, 2013 WL 3914484, at \*10 (5th Cir. July 30, 2013) (“A cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call.” “Cell phone users, therefore, understand that their service providers record

squarably addressed the issue; however, in a recent unpublished opinion it found no plain error in the district court's admission of cell site location records disclosed pursuant to a subpoena for which there was no finding of probable cause. *See United States v. Pascual*, 502 F. App'x. 75, 80 (2d Cir. Nov. 13, 2012). The Second Circuit noted that the case on which the defendant relied in arguing that a warrant was required was "at the very least in some tension with prevailing case law," and thus there could be no plain error "when no governing precedent from this Court or the Supreme Court required exclusion, and the general principles adopted by those courts pointed the other way." *Id.* (citing *Smith*, 442 U.S. at 742-44 (holding that a customer has no reasonable expectation of privacy in dialed telephone number which were conveyed to the telephone company) and *Miller*, 425 U.S. at 443 (holding that Fourth Amendment did not "prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."))).

*Pascual*, although of no precedential value, reflects the Second Circuit's probable approach to the disclosure of real time GPS data using the voluntary disclosure doctrine.

---

their location when they use their phones at least to the same extent that the landline users in *Smith* understood that the phone company recorded the numbers they dialed."); *In re Smartphone Geolocation Data Application*, 2013 U.S. Dist. LEXIS 62605, at \*45 (E.D.N.Y. May 1, 2013) ("Cell phone customers . . . convey geolocation data to their telephone carriers, and cannot possibly labor under the belief that their location is somehow kept secret from telecommunications carriers and other third parties. Under existing law, then, a user does not have a reasonable expectation of privacy as to geolocation data."); *United States v. Graham*, 846 F. Supp. 2d 384, 401 (D. Md. 2012) (observing that *Smith* "cautions against any assumption of ignorance on the part of cellular customers. Additionally, any assumption of ignorance is belied by Sprint/Nextel, Inc.'s privacy policy, which informs its customers that it collects location data"); *In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113, 121 (E.D.N.Y. 2011) ("Public ignorance as to the existence of cell-site-location records . . . cannot long be maintained.") *with In Re Application of the United States for Order Directing Provider of Elec. Commc'n Serv. To Disclose Records to Gov't*, 620 F.3d 304, 317 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."); *Earls*, 2013 WL 3744221, at \*11 (N.J. July 18, 2013) (deciding that state constitution recognizes an expectation of privacy in cell phone location data and noting that "[w]hen people make disclosures to phone companies and other providers to use their services, they are not promoting the release of their personal information to others").

Under *Smith*, “[a]ll [cell phone] users realize that they must ‘convey’ [the locations of their devices] to the [cell phone] company, since it is through [cell phone] company switching equipment that their calls are completed.” *Smith*, 442 U.S. at 742. Under *Miller*, “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.” *Miller*, 425 U.S. at 443. As one court has observed, a cell phone user voluntarily discloses his or her cell phone’s location in the ordinary course of its use:

[I]t is clearly within the knowledge of cell phone users that their telecommunications carrier, smartphone manufacturer and others are aware of the location of their cell phone at any given time. After all, if the phone company could not locate a particular cell phone, there would be no means to route a call to that device, and the phone simply would not work. Given the notoriety surrounding the disclosure of geolocation [data] . . . cell phone users cannot realistically entertain the notion that such information would (or should) be withheld from federal law enforcement agents searching for a fugitive.

As to control by the user, all the known tracking technologies may be defeated by merely turning off the phone. Indeed—excluding apathy or inattention—the only reason that users leave cell phones turned on is so that the device can be located to receive calls. Conversely, individuals who do not want to be disturbed by unwanted telephone calls at a particular time or place simply turn their phones off, knowing that they cannot be located.

*In re Smartphone Geolocation Data Application*, 2013 U.S. Dist. LEXIS 62605, at \*46-47 (internal citations omitted); see also *In Re Application of the United States of American for Historical Cell Site Data*, 2013 WL 3914484, at \*10 (5th Cir. July 30, 2013) (overruling *In Re Application of the United States for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D. Tex. 2010) and concluding that cell phone users are generally aware that historical cell site location data is collected and maintained and may be turned over to third parties); *In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113, 121 (E.D.N.Y. 2011) (rejecting the assertion that cell site information is not voluntarily conveyed to the service

provider because it “relies too heavily on cell-phone users remaining unaware of the capacities of cellular technology, a doubtful proposition in the first place”). Accordingly, as a general proposition, cell phone location data is information a cell phone user voluntarily discloses to a third party in order to enable the cell phone user to send and receive calls. *Smith* and *Miller* thus support a conclusion that a cell phone user generally has no reasonable expectation of privacy in cell site information communicated for the purpose of making and receiving calls in the ordinary course of the provision of cellular phone service.

Here, however, disclosure of Defendant’s cell phone data location did not occur in the ordinary course of providing cellular phone service. Rather, it occurred pursuant to a special, surreptitious procedure not available to the general public, initiated solely by law enforcement, without notice or any volitional activity by Defendant other than having his phone in the “on mode.” As a general proposition, cell phone users do not expect their cell phones to be pinged in the ordinary course of business. In this respect, the instant case is distinguishable from *Smith* and *Miller* as pinging simply is not part and parcel of the provision of cellular phone service. This court, however, need not resolve the thorny question of whether an individual *generally* maintains a subjective expectation of privacy in his or her real time location data where that information is obtained exclusively through pinging because any subjective expectation of privacy in such circumstances must give way where, as here, there is a true emergency.

#### **4. Expectations of Privacy in the Face of an Emergency.**

As a threshold proposition, in 2011, cell phone users, like the telephone users in *Smith* and *Miller*, were generally aware that their cell phones may contain a location device that can be accessed by law enforcement and other first responders in the event of an emergency. Indeed, by 2011, federal law mandated that cell phones provide enhanced location services whenever 911 services were accessed.<sup>6</sup> In turn, in 2011, 18 U.S.C. §

---

<sup>6</sup> See Wireless Communications and Public Safety Act of 1999, 47 U.S.C. §§ 615a-615c. Section 615a-1 of the Act states that: “It shall be the duty of each IP-enabled voice service

2702(c)(4) of the Stored Communications Act authorized cell phone service providers to disclose without a warrant “a record or other information pertaining to a subscriber to or customer of [cell phone] service . . . to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.” Congress thus deemed it reasonable to subordinate any individual privacy interest in cell phone location information to society’s more compelling interest in preventing an imminent threat of death or serious bodily injury. “Because there is a ‘strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is “reasonable,” “[o]bviously the Court should be reluctant to decide that a search thus authorized by Congress was unreasonable and that the Act was therefore unconstitutional.” *United States v. Watson*, 423 U.S. 411, 416 (1976) (quoting *United States v. Di Re*, 332 U.S. 581, 585 (1948)).

Defendant nonetheless argues that the Stored Communications Act does not authorize the disclosure of real time GPS location data in the event of an emergency because real time location data is not “a record or other information” within the meaning of the Act. *See* Doc. 56 at 11-13.<sup>7</sup> The Government more persuasively argues that the

---

provider to provide 9-1-1 service and enhanced 9-1-1 service to its subscribers in accordance with the requirements of the Federal Communications Commission, as in effect on July 23, 2008 and as such requirements may be modified by the Commission from time to time.” Section 615b(10) defines “enhanced 9-1-1 service” as “the delivery of 9-1-1 calls with automatic number identification and automatic location identification, or successor or equivalent information features over the wireline E911 network (as defined in section 9.3 of the Federal Communications Commission’s regulations (47 C.F.R. § 9.3) as of July 23, 2008) and equivalent or successor networks and technologies.”

<sup>7</sup> The court rejects Defendant’s invitation to adopt the approach some courts have taken in holding that the acquisition of cell tower site information effectively converts an individual’s cell phone into a “tracking device” which requires a warrant. Federal law governs government “installation of a mobile tracking device,” 18 U.S.C. § 3117 (emphasis supplied), which simply does not occur in the pinging process in which the government accesses a cell phone’s inherent capabilities to obtain location data without installing any device in or on the cell phone itself. *See United States v. Powell*, 2013 WL 1876761, at \*13 (E.D. Mich. May 3, 2013) (“Moreover, a cell phone is not a ‘tracking device’ as defined by 18 U.S.C. § 3117. First, a cell phone is not a

Act authorizes the disclosure of real time location data by broadly authorizing the disclosure of “other information,” presumably in recognition of the fact that in a true emergency, limits on the types of information available to prevent or minimize the emergency should be sparing. *See United States v. Gilliam*, 2012 WL 4044632, at \*1-2 (S.D.N.Y. Sept. 12, 2012) (holding request for “cell site information as well as information about [defendant’s] precise location” based upon “an exigent situation involving ‘immediate danger of death or serious bodily injury’ involving the prostitution of a missing child” was “justified under the Stored Communications Act”). This interpretation of “other information” is buttressed by the Stored Communications Act’s authorization to a cellular phone service provider to “divulge the contents of a communication . . . to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.” 18 U.S.C. § 2702(b)(8). It would be anomalous to permit disclosure of the otherwise sacrosanct *contents* of cell phone communications to prevent an emergency, but prohibit disclosure of the cell phone’s *location* as an unjustified intrusion on privacy. Defendant identifies no societal interests which would be advanced by that strained interpretation of the Act.

Moreover, even in the unlikely event that Defendant is correct in arguing that law enforcement and Sprint Nextel violated the emergency provisions of the Stored Communications Act, any violation would not give rise to a Fourth Amendment violation

---

government-owned-and-installed device. Instead, it is a personal communications device that an individual purchases and owns. The statutory language of § 3117 specifically contemplates government installation: “[i]f a court is empowered to issue a warrant or other order for the *installation* of a mobile tracking device[.]”. 18 U.S.C. § 3117(a)); *In re Application of the United States for an Order*, 411 F. Supp. 2d 678, 681 (W.D. La. 2006) (concluding “[t]racking devices are devices that are ‘installed’ at the request of the Government” and thus “[a] cellphone is not a tracking device as that term is commonly understood.”); *In re Smartphone Geolocation Data Application*, 2013 U.S. Dist. LEXIS 62605 at 57 (“[C]onstruing ‘tracking device’ to encompass a cell phone is simply illogical and unworkable in this context.”); *In re Application for an Order Authorizing the Extension and use of a Pen Register Device*, 2007 WL 397129, at \*2 (E.D. Cal. Feb. 1, 2007) (holding 18 U.S.C. § 3117(b) “does not include the acquisition of cell site information in the terms of ‘tracking device.’”).

that did not otherwise exist. *See City of Ontario v. Quon*, 130 S. Ct. 2619, 2632 (2010) (noting that even if there was a violation of the Shared Communications Act, “it does not follow that petitioners’ actions were unreasonable. Respondents point to no authority for the proposition that the existence of statutory protection renders a search *per se* unreasonable under the Fourth Amendment. And the precedents counsel otherwise.”) (citing *Virginia v. Moore*, 553 U.S. 164, 168 (2008) (search incident to an arrest that was illegal under state law was reasonable); *California v. Greenwood*, 486 U.S. 35, 43 (1988) (rejecting argument that if state law forbade police search of individual’s garbage the search would violate the Fourth Amendment)); *see also United States v. Kington*, 801 F.2d 733, 737 (5th Cir. 1986) (analyzing the Right to Financial Privacy Act and holding that “[t]he rights created by Congress are statutory, not constitutional.”).

Sprint Nextel’s general terms and conditions of service and its privacy policies underscore the conclusion that Defendant did not retain an actual subjective expectation of privacy in his real time location data in an exigent situation. In 2011, Sprint Nextel advised its customers that it collects information regarding the location of its customers’ cell phones while in use, it generally knows where those cell phones are, and it “may access, monitor, use or disclose [that] personal information or communications to do things like: . . . comply with the law or respond to lawful requests or legal process . . . [and] respond to emergencies[.]” Gov’t Ex. 3 at 2. Defendant thus clearly had notice that disclosure of his cell phone’s location to law enforcement may occur in order to respond to an emergency. Contrary to Defendant’s argument, this emergency was not limited to his own safety but, by its terms, extended to a threat to the safety of others.

Finally, in this case, there can be no reasonable dispute that the pinging of Defendant’s cell phone was occasioned by an “exigent situation.” At the time of the pinging, law enforcement had reason to believe that Melissa Barratt was the victim of a homicide and that whoever had committed this “execution style” crime had recently left the scene with the homicide weapon. Law enforcement also had recent, firsthand information that Ms. Barratt feared that Defendant would kill or harm her if she

cooperated with law enforcement. She told law enforcement that Defendant was armed, had an array of weapons, and had engaged in similar crimes in the past.

Each of law enforcement's controlled buys with Defendant had recently occurred in the nearby Brattleboro area through the use of confidential informants. These informants knew Defendant well enough to contact him by one or both of his cell phone numbers. They were thus likely to be individuals who had encountered Defendant on more than a single, remote, or passing occasion. Defendant, in turn, was likely to know the confidential informants' identities and potential whereabouts and how they might be found. Law enforcement knew that Defendant had access to at least two motor vehicles. They also knew he had access to weapons and had a criminal history that included assaults. Based upon this information, law enforcement held a legitimate, good faith belief that Defendant must be apprehended immediately to ensure that confidential informants and undercover narcotics agents would not be exposed to an imminent risk of death or serious bodily injury in the event that Defendant was the person who killed Ms. Barratt in retaliation for her recent statements regarding his criminal activities to the police. If the motive for the Barratt homicide was to silence a cooperator, it could extend to the confidential informants as well.

Although law enforcement considered obtaining a search warrant for Defendant's cell phone data, past experience reasonably supported a conclusion that it would be approximately six hours before a warrant could be obtained from a state court judge and several days or weeks thereafter before cell phone location data would be provided by the cellular service provider. By that time, the data might have forensic value, but it could not be used to prevent an emergency. Law enforcement considered other options, but reasonably concluded that they were not likely to lead to Defendant's immediate apprehension.

Based upon the totality of the circumstances, because Defendant was on notice that disclosure of his real time location information to law enforcement may occur in the event of an "emergency," he cannot be deemed to have retained an actual subjective



expectation of privacy in the circumstances of this case. Even in the unlikely event that he held such a belief, it is not one society is prepared to accept as reasonable.<sup>8</sup> Such an approach would safeguard as “private” the use of available technology to prevent an emergency even if the alleged privacy interest put lives at stake. No court has reached this conclusion, nor would such a conclusion be reasonable under the Fourth Amendment. *See Michigan v. Fisher*, 558 U.S. 45, 47 (2009) (noting that the Supreme Court has repeatedly held that “the ultimate touchstone of the Fourth Amendment . . . ‘is reasonableness.’”) *Id.* (internal citations omitted).

Accordingly, in the circumstances of this case, no “search” of Defendant’s cell phone occurred for purposes of the Fourth Amendment and Defendant’s motion to suppress is DENIED on that basis.

**C. If a Fourth Amendment Search Occurred, Exigent Circumstances and a Reasonable, Good Faith Reliance Upon Applicable Law Render the Absence of a Warrant Reasonable and Suppression Unwarranted.**

In the event that it is determined that a “search” of Defendant’s cell phone occurred for purposes of the Fourth Amendment, law enforcement’s failure to obtain a warrant remained reasonable in this case because of the presence of exigent circumstances and a reasonable, good faith reliance upon applicable law. Suppression is therefore not warranted.

**1. Exigent Circumstances Authorized the Warrantless Search.**

The test to determine exigent circumstances “is an objective one that turns on . . . the totality of circumstances confronting law enforcement agents in the particular case.”

---

<sup>8</sup> In arguing that society is prepared to accept as reasonable a general subjective expectation of privacy in cell phone location data, Defendant relies on principles developed by the Digital Due Process Coalition and five different bills proposed (but not passed) in the Senate and House that would govern and limit disclosure of cell site location information, as well as two additional bills addressing “geolocational privacy” that have been introduced since he filed his motion. Although Defendant accurately observes that there appears to be concern in some sectors regarding the government’s procurement and use of real time location information, against the backdrop of existing and recent federal legislation which permits such information to be obtained and used in the precise circumstances of this case, societal expectations cannot be said to favor maintaining location data as private in an exigent situation.

*United States v. MacDonald*, 916 F.2d 766, 769 (2d Cir. 1990) (en banc). The question is whether “the facts, as they appeared at the moment of entry, would lead a reasonable, experienced officer, to believe that there was an urgent need to render aid or take action.”” *United States v. Simmons*, 661 F.3d 151, 157 (2d Cir. 2011) (quoting *United States v. Klump*, 536 F.3d 113, 117-18 (2d Cir. 2008)). The Second Circuit has identified six factors to assist in determining whether there are exigent circumstances:

- (1) the gravity or violent nature of the offense with which the suspect is to be charged; (2) whether the suspect “is reasonably believed to be armed”; (3) “a clear showing of probable cause . . . to believe that the suspect committed the crime”; (4) “strong reason to believe that the suspect is in the premises being entered”; (5) “a likelihood that the suspect will escape if not swiftly apprehended”; and (6) the peaceful circumstances of the entry.

*United States v. Reed*, 572 F.2d 412, 424 (2d Cir. 1978) (quoting *Dorman v. United States*, 435 F.2d 385, 392-93 (D.C. Cir. 1970)). It has “consistently emphasized that [these] factors are intended not as an exhaustive canon, but as an illustrative sampling of the kinds of facts to be taken into account. Sometimes the presence of a solitary factor suffices, [or] alternatively, a combination of several.” *MacDonald*, 916 F.2d at 770.

Here, the exigent circumstances consisted of an “execution style” homicide (a violent and extremely serious offense) that appeared to have taken place that morning. The person whom committed the homicide was believed to be armed. Defendant had recently been identified by Ms. Barratt as a person who was likely to kill or harm her if he knew she was making statements to the police. Although law enforcement personnel believed they lacked probable cause to arrest Defendant for the Barratt homicide, Defendant remained law enforcement’s “primary suspect.” Law enforcement reasonably believed there was a serious public safety risk if Defendant was not swiftly apprehended. Cell phone pinging presented a peaceful and apparently lawful means of quickly discerning Defendant’s location in order to maintain at least surveillance over him and to enhance law enforcement’s ability to effect an expeditious and safe arrest. *See Dorman*, 435 F.2d at 392 (“Delay in arrest of an armed [suspect] may well increase danger to the

community meanwhile, or to the officers at time of arrest. This consideration bears materially on the justification for a warrantless [search].”).

At the time, law enforcement also had a substantial and legitimate interest in apprehending a primary suspect in the Barratt homicide when any evidence of the alleged crime (such as gun powder residue, the homicide weapon, DNA, blood traces, shoe imprints, tire imprints, and other evidence) could still be obtained. Courts, including the Supreme Court, have recognized that the need to obtain and preserve critical evidence in the investigation of a serious crime constitutes “exigent circumstances” which renders the failure to obtain a warrant reasonable under the Fourth Amendment. *See Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011) (“[T]he need ‘to prevent the imminent destruction of evidence’ has long been recognized as a sufficient justification for a warrantless search.”) (quoting *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006)); *United States v. Moreno*, 701 F.3d 64, 74 (2d Cir. 2012) (concluding exigent circumstances justified warrantless entry into motel room when suspect’s “unusual behavior . . . raised a legitimate concern that she would attempt to destroy or discard the drugs that the agents had probable cause to believe were inside”); *Simmons*, 661 F.3d at 157 (“An[] exigency is the need to prevent the imminent destruction of evidence.”); *MacDonald*, 916 F.2d at 770 (affirming “district court’s finding that the [government] agents were confronted by an urgent need to prevent the possible loss of evidence” in light of “the ease with which the suspects could have disposed of the cocaine by flushing it down the toilet, and the possibility that the prerecorded five dollar bill used . . . in the undercover buy would be lost if the ongoing drug transactions were permitted to continue while the [government] agents sought a warrant”). Here, the warrant process would take days if not weeks to unfold.

For the foregoing reasons, the court concludes that exigent circumstances alone rendered the warrantless search of Defendant’s cell phone location reasonable, under the Fourth Amendment. *See MacDonald*, 916 F.2d at 770.

## **2. Good Faith, Reasonable Reliance on Applicable Law Renders Suppression Unwarranted.**

In addition to exigent circumstances, law enforcement had a good faith, reasonable belief that applicable law authorized the pinging of Defendant's cell phone in the circumstances of this case. In *Illinois v. Krull*, 480 U.S. 340 (1987), the Supreme Court concluded that its holding in *United States v. Leon*, 468 U.S. 897 (1984), "that the Fourth Amendment exclusionary rule does not apply to evidence obtained by police officers who acted in objectively reasonable reliance upon a search warrant issued by a neutral magistrate, but where the warrant was ultimately found to be unsupported by probable cause," should be extended to instances in which "officers act in objectively reasonable reliance upon a *statute* authorizing warrantless administrative searches, but where the statute is ultimately found to violate the Fourth Amendment." *Krull*, 480 U.S. at 342. As the *Krull* Court pointed out,

The application of the exclusionary rule to suppress evidence obtained by an officer acting in objectively reasonable reliance on a statute would have as little deterrent effect on the officer's actions as would the exclusion of evidence when an officer acts in objectively reasonable reliance on a warrant. Unless a statute is clearly unconstitutional, an officer cannot be expected to question the judgment of the legislature that passed the law. If the statute is subsequently declared unconstitutional, excluding evidence obtained pursuant to it prior to such a judicial declaration will not deter future Fourth Amendment violations by an officer who has simply fulfilled his responsibility to enforce the statute as written. To paraphrase the Court's comment in *Leon*: "Penalizing the officer for the [Congress'] error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations."

*Id.* at 349-50 (quoting *Leon*, 468 U.S. at 921); *see also United States v. McCullough*, 2013 WL 1729712, at \*1 (2d Cir. Apr. 23, 2013) ("Under the good faith exception to the exclusionary rule, evidence obtained by an officer acting in objectively reasonable reliance on a statute will be admitted unless the statute was "clearly unconstitutional" at the time that the officer obtained the evidence") (citing *Krull*, 480 U.S. at 349-50).

Here, the Stored Communications Act has not been ruled unconstitutional, nor does Defendant challenge its constitutionality. Moreover, the court has specifically found that, in this case, law enforcement and Sprint Nextel acted reasonably and in good faith in relying upon the Act's provisions authorizing cell phone pinging in an exigent situation. As a result, even if a Fourth Amendment violation could be found, suppression would not be warranted as it would serve no deterrent purpose. *See Davis v. United States*, 131 S. Ct. 2419, 2427-28 (2011) ("But when the police act with an objectively "reasonable good-faith belief" that their conduct is lawful, or when their conduct involves only simple, "isolated" negligence, the "deterrence rationale loses much of its force," and exclusion cannot "pay its way.") (internal quotation marks and citations omitted); *see also United States v. Takai*, 2013 WL 1831993, at \*7 (D. Utah Apr. 30, 2013) (ruling that based upon the emergency provisions of the Stored Communication Act, "even if the court were required to find that [law enforcement] acquired the CSLI [cell site location information] in violation of Defendant's Fourth Amendment rights, the *Leon* good faith exception, as further applied by *Illinois v. Krull*, 480 U.S. 340, 349 (1987), would remove suppression as an available remedy"); *Graham*, 846 F. Supp. 2d at 406 (holding that it is "objectively reasonable for law enforcement to rely on the Stored Communications Act" in obtaining historical cell site location information and thus suppression was not warranted). Law enforcement's good faith, reasonable reliance on the applicable law in pinging Defendant's cell phone without a warrant is thus sufficient grounds to deny Defendant's motion to suppress.

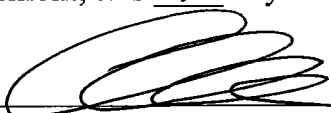
In summary, the court has found that no Fourth Amendment "search" occurred in this case. Even if a search occurred, suppression of the evidence gleaned from the search is not warranted. Accordingly, the court does not address the government's further arguments that the automobile exception and the inevitable discovery doctrine rendered any search of Defendant's cell phone constitutionally valid.

### CONCLUSION

For the foregoing reasons, Defendant's Motion to Suppress Evidence Based on the Government's Warrantless Use of Real-Time Cell Phone Location Information (Doc. 38) is DENIED.

SO ORDERED.

Dated at Rutland, in the District of Vermont, this 7<sup>th</sup> day of August, 2013.

  
\_\_\_\_\_  
Christina Reiss, Chief Judge  
United States District Court